International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

The Security Threats in Cloud Architecture- A Review

Simanjot Kaur[1], Anurag Singh Tomar[2]

[1, 2]Department of CSE, Lovely Professional University, Jalandhar, Punjab, India

Abstract: ***The cloud computing architecture in which third party, virtual machine and cloud service provider are involved for data uploading and downloading. The security, access controls are the various issues which are in the cloud architecture. The security is the main issue which reduce the performance of cloud architecture. Among security attacks zombie attack is the most advance type of attack. This attack reduces network performance in terms of delay and bandwidth consumption. In the zombie attack, some malicious nodes may join the network which spoof data of the legitimate and zombie nodes start communicate with virtual machine on the behalf of legitimate node. In this work, enhancement will be proposed in access control scheme which will detect malicious nodes from the network and isolate then from the cloud architecture.***

Keywords: Cloud Computing; Security; Mutual Authentication Schemes

1. Introduction

1.1 Cloud Computing

Cloud computing is the recently evolved computing terminology based on the utility and the consumption of computing resources. Cloud computing provides shared resources, software [6] and the information to the various computers and devices on demand because cloud computing is an internet based.For example, drop box and google. Cloud computing provides the three services that are:-

a) Infrastructure as a Service (IaaS)
It is defined as the customer can provision the computing resources such as processing, storage and networking on demand such as amazon web services.

b) Platform as a Service (PaaS)
It is defined as the customer gets an open platform and solution stack, where he/she can deploy the application developed in application in language given by provider such as windows azure.

c)Software as a Service (SaaS)
It is defined as the customer can run applications in cloud and can access the applications through various clients including browsers, mobile devices and Salesforce.com etc.

1.2 Challenges of Cloud Computing

There are various challenges in the cloud computing such as:

a) Privacy and Security
Cloud computing provides more security and privacy. It can protect system from various attacks by using various security applications, encrypted sile systems etc.

b) Downtime and Accessibility
Services Quality does not have cooperated when your data in cloud. Accessing your data when you need it is basic constraint from many organisations. The main challenge with the cloud is that the data is accessed via the internet rather than local connection. So, when the internet connection is down, then the cloud services are also down and data cannot be accessed by anyone.

c) Portability and Interoperability
It is the one of the most challenge in cloud computing. To preserve their ability to change vendors in the future, agencies may attempt to avoid platforms or technologies that lock customers in particular product

1.3 Cloud Computing Security

Network security, information security and many other security types like the computer security together make the term "Cloud Security. It gives the wide set of technologies, rules and controls that are used to provide the security to data and several applications that exist with the cloud computing environment. Security is the most concerning point to any service. Only security ensures the privacy and integrity the cloud data. There are many types of security issues exist:

- Data Loss
- Downtimes
- Phishing
- Password Cracking
- Botnets and Other Malware

2. Literature Review

In 2012, Chirag Modi et al [1]include the survey on various security issues (and solutions at different layers of cloud Computing. In this paper, they discuss the various threats to cloud computing are:

- Changes to business model.
- Insecure application program interface.
- Malicious insiders.
- Data loss.
- Data leakage.
- Service hijacking.

Authors define the different types of attacks on cloud computing such as zombie attack, Man in the middle attack [8], spoofing attack, service injection attack, phishing Attack

and backdoor channel attack. They detect these attacks by using Intrusion detection system, Intrusion prevention system, using secure hypervisors, by proper configuration of secure socket layer and detect the mails that are spam and providing better authorization and authentication. It provides robust separation among different virtual machines to detect these attacks. They show the issues of the security at the dissimilar layers in cloud. Different layers are cloud user layer, cloud service provider layer, cloud virtualization layer and data storage and internal network layer.

One solution of this to use the XML signature and XML encryption to increases the security of browser. They also used the simple object access protocol. They also use access control policy language (ACPL) for describes the policies in cloud and also use access control oriented ontology system (ACOOS) to provide semantic information. In this, main concept is building trust on the cloud in future research area.

In 2013, Iti Raghav et al [2] includes the different types of clouds and its five essential features are rapid elasticity, resource pooling, Broad network access, scalability and on demand service. It includes the three services of cloud computing are Infrastructure as a Service [6], Platform as a Service and Software as a Service. In this paper, use the intrusion detection system (IDS) to protect the network and the computer from different attacks. The main aim of IDS is to detect the various attacks and produce a proper and secure response. IDS is capable of distinguish between the insider attack and the external attacks. There are twoIntrusion detection systems are used to detect the attacks:

- Host Based Intrusion Detection System (HIDS)
- Network Based Intrusion Detection System (NIDS)

There are two different approaches for intrusion prevention System are: host based approach, network based approach. It increases the detection rate. But, it has not been provided desired features of security. So, to increases the detection rate by implementing the hybrid cloud. Further work will be done by a third party IDS provider on cloud IDS approach.

In 2014, Jen-Ho Yang et al [3] in architecture of Cloud Computing, authentication scheme based on user is an essential security tool since it offers authentication based on accounting for the clients of cloud. They proposed user authentication scheme centred on new ID. Before this proposed scheme, there are many authentication scheme based on the ID like remote user authenticate scheme based on Dynamic ID, its permits clients to change and select the password free of cost and do not keep [7] some verifier table. In this das, demanded that this scheme is fully secure against various attacks. But Wang notices that it is run on the insecure channel, so it is unsecure [9]. Then the Improvement has been done on the existing scheme user authentication scheme centred on new ID. But, there are many security problems, security flaws, high communication and computational cost are found in these schemes. Due to these problems, yang and pie propose a new scheme and in this scheme includes three different parts:

- User
- Server
- ID Provider

Each of these has different responsibility. In this novel scheme, they use the two phase's, first phase is that in which the user register and second is that phase in which both the user and the server verify its identity earlier communication starts. They use one way hash function and XOR to reduce the computational and communication cost. This scheme can be applied on the multiple servers so the client preserve single message of authentication to sign in several virtual machine and they also analyze the performance amongst technique which is planned and existing scheme and also show the security analysis of different attacks such as replay attack, impersonation attack, insider attack and outsider attack.

In 2014, D. Nimmy K et al [4] includes an essential technology of cloud computing is proper authentication that defines connection to outside environment are mutual and risks are high. They planned propose a new mutual authentication based scheme where the user and the cloud server can authenticate one another. In this, they use the steganography to cover the image and data and also use the secret key that is shared between both the cloud server and user.

One of the main challenges is mutual authentication because both the user and server can authenticate themselves before the communication begins. There are various methods of authentication like plain password etc.

The various existing schemes such as user authentication scheme based time bound, mutual authentication scheme based new ticket [10] that using smart cards , strong and reliable user authentication scheme [11] in which each user and the server has proven its identity. But in these schemes has found many security problems and the novel mutual authentication scheme for cloud computing using secret sharing and steganography has been proposed. In the proposed scheme, different phases are used that are:

- Registration Phase
- Login Phase
- Mutual Authentication Phase
- Password Change Phase

This scheme has also show the security analysis of different attacks and analyses the resistivity of this scheme to various attacks such as replay attack, masquerade attack, DoS attack, insider attack. A significant scheme based on mutual authentication for cloud computing with several features of security such as the user and cloud server shared the session key, change the password and mutual authentication.

Authors suggest that the novel technique based on scheme can use the out of band (OOB) authentication to provide the interaction with human that builds the scheme stronger and none use of any software and the hardware for the end users. But this paper has not shown any comparison related to performance with the schemes that already exists. This scheme can oppose many widespread attacks such as masquerade attack, insider attack, replay attack and DoS attack. But this propose scheme do not resist any other attack such as zombie attack and do not detect the zombie nodes from the cloud network.

In 2015, E. Prachi Deshpande et al [5] Cloud computing is a collection of sources in order to enable resource sharing in terms of scalability, services that are delivered on demand over the network. Classification and analyze on different threat related to security in the environment of cloud computing alongside with classification of intrusion detection system in short term. Different threats are commenced onto cloud private model and finding and avoidance carried out through snort technique. The snort is freely available which usages the procedure related to name for identifying malicious users.

Snort is free and widely usages. Its platform like GNU, windows, Linux and regularly updated. Snort Captures data packets related to network, then check contents through by default well-known packet pattern to some association. Basically, the way of snort exist inline and protects system. To analyze efficiency by using the two threats of security: the Flooding attack and Port scan attack. Threats associated with security such as port scan and flooding sprang onto open Nebula frontend to authenticate the cloud behaviour with the help of hping. In future work, we proposed deploy and design of comprehensive IDS for detection of threats of security with a capacity.

3. Problem Formulation

Due to number of reasons, Cloud computing unavoidably presents novel challenging threats of security. Initially, Cloud Computing is not a data warehouse of third party. The data that is stored in the cloud might be often insertion, appending modification, deletion and reordering etc by the users of cloud. Since several types of data are stored in the cloud of every user, the main problem of confirming data accuracy that is stored in the cloud becomes more challenging.

Analysis of performance and security shows that the technique that is planned is extremely resourceful and hardy in contradiction of failure of Byzantine, server crashing attacks and malicious data changing attack.In this work, we will enhance the proposed technique to detect and isolate zombie attack in cloud computing. To prevent the zombie attack, novel technique will be proposed which is based on the server identification. Before present its credentials to the server, legitimate client will ask the server for its credentials. If the sever credentials are verified by the client then further process will proceed otherwise algorithm will halt.

4. Conclusions

In this work, it is been concluded that access control scheme is efficient type of scheme for cloud architecture. In this scheme access control lists are maintained by the third party to provide access to users. In the architecture, some malicious nodes may join the network which is responsible to trigger zombie attack in the network. These zombie nodes can spoof the information of the legitimate nodes and communicate with virtual machine on the behalf of legitimate nodes. This will leads to reduction in network performance in terms of delay and bandwidth consumption. In further work, improvement will be proposed based on mutual authentication scheme for the detection malicious nodes from the network.

References

[1] Modi, Chirag, Dhiren Patel, Bhavesh Borisaniya, Avi Patel, and Muttukrishnan Rajarajan "A survey on security issues and solutions at different layers of Cloud computing", The Journal of Supercomputing 63, pp. 561-592, 2012.
[2] Raghav, Iti, Shashi Chhikara, and Nitasha Hasteer "Intrusion Detection and Prevention in Cloud Environment: A Systematic review", International Journal of Computer Applications 68, pp. 7-11, 2013.
[3] Jen-Ho Yang, and Pei-Yu Lin "An ID-Based User Authentication Scheme for Cloud Computing", Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 98-101, 2014.
[4] Nimmy K, and M. Sethumadhavan "Novel Mutual Authentication Protocol for Cloud Computing using Secret Sharing and Steganography", Fifth International Conference on the Applications of Digital Information and Web Technologies (ICADIWT) – Bangalore, India, pp. 101-106, 2014.
[5] Prachi Deshpande, S.C. Sharma, and P. Sateeshkumar "Security Threats in Cloud Computing", International Conference on Computing, Communication and Automation (ICCCA2015), pp. 632-635, 2015.
[6] Tiwari, Pradeep Kumar, and Bharat Mishra "Cloud Computing Security Issues, Challenges and Solution", International Journal of Emerging Technology and Advanced Engineering, pp. 306-310, 2012.
[7] M. L. Das, A. Saxena, and V. P. Gulati, "A dynamic ID-based remote user authentication scheme" , IEEE Transactions on Consumer Electronics, vol. 50, no. 2, pp. 629-631, 2004.
[8] Singh, Ajey, and Maneesh Srivastava "Overview of attacks on cloud computing", International Journal of Engineering and Innovative Technology (IJEIT), pp.1-4, 2012.
[9] Y. Wang, J. Liu, F. Xiao, and J. Dan, "A more efficient and secure dynamic ID-based remote user authentication scheme", Computer Communications, vol.32, no.4, pp. 583-585, 2009.
[10] Z. Hao, S. Zhong, and N. Yu, "A Time-Bound Ticket-Based Mutual Authentication Scheme for Cloud Computing", Int. J. of Computers, Communications & Control, vol. VI (2011), No. 2 (June), pp. 227- 235, 2006.
[11] A. J. Choudhury, P. Kumar, M. Sain, H. Lim, and H. Jae-Lee, "A Strong User Authentication Framework for Cloud Computing," in Services Computing Conference (APSCC), IEEE Asia-Pacific, pp. 110–115, 2011.